Social Data

WOODROW HARTZOG*

As online social media grow, it is increasingly important to distinguish between the different threats to privacy that arise from the conversion of our social interactions into data. One well-recognized threat is from the robust concentrations of electronic information aggregated into colossal databases. Yet much of this same information is also consumed socially and dispersed through a user interface to hundreds, if not thousands, of peer users.

In order to distinguish relationally shared information from the threat of the electronic database, this essay identifies the massive amounts of personal information shared via the user interface of social technologies as "social data." The main thesis of this essay is that, unlike electronic databases, which are the focus of the Fair Information Practice Principles (FIPPs), there are no commonly accepted principles to guide the recent explosion of voluntarily adopted practices, industry codes, and laws that address social data.

This essay aims to remedy that by proposing three social data principles—a sort of FIPPs for the front-end of social media: the Boundary Regulation Principle, the Identity Integrity Principle, and the Network Integrity Principle. These principles can help courts, policymakers, and organizations create more consistent and effective rules regarding the use of social data.

TABLE OF CONTENTS

---

* Assistant Professor, Cumberland School of Law at Samford University; Affiliate Scholar, The Center for Internet and Society at Stanford Law School. The author would like to thank Ryan Calo, Michael Froomkin, Eric Goldman, Airi Lampinen, Geoffery Manne, Evan Selinger, Fred Stutzman, Peter Swire, the Cumberland School of Law faculty, and the participants of the Ohio State Law Journal's Symposium on the Second Wave of Global Privacy Protection and participants of the Third Annual Internet Law Works-in-Progress Series.

I. INTRODUCTION

The predominant response to the industrial-scale collection and use of personal information has been to structure both voluntary and compulsory privacy protections around a set of commonly accepted principles known as the Fair Information Practice Principles, often referred to as the FIPPs.[1] While the FIPPs have played an important role in the systematic protection of personal data stored in electronic databases, they are woefully insufficient for the public-facing side of a different but related technology: social media.[2]

Social media is defined broadly here as any digital communication technology utilizing the Internet to connect people for social reasons. Social media and electronic databases represent two distinct threats that are often conflated. Social media are certainly part of the "big data" phenomenon.[3] It is

---

[1] *See, e.g.*, Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239, 242 (2013); *see also* Robert Gellman, *Fair Information Practices: A Basic History, Version 1.92*, BOB GELLMAN 1 (June 24, 2013), http://bobgellman.com/rg-docs/rg-FIPShistory.pdf (discussing the development of the Fair Information Practices in the United States).

[2] The term "social media" is notoriously difficult to define. At its broadest, it can refer to every Internet-based communication technology. Eric Goldman, *Big Problems in California's New Law Restricting Employers' Access to Employees' Online Accounts*, FORBES (Sept. 28, 2012, 12:39 PM), http://www.forbes.com/sites/ericgoldman/2012/09/28/big-problems-in-californias-new-law-restricting-employers-access-to-employees-online-accounts/ (noting that laws proposed to regulate social media instead cover "effectively all digital content and activity, both on the Internet and stored in local storage devices, not just social media" and that "it's not possible to define 'social media' as a subset of the Internet ecosystem"). However, a more circumscribed definition is offered by danah boyd and Nicole Ellison for the related term "social network site," as "web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system." danah m. boyd & Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship*, 13 J. COMPUTER-MEDIATED COMM. 210, 211 (2008).

[3] *See* VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 91–94 (2013); Julie E. Cohen,

hardly a secret that Facebook, Twitter, and other social media have robust concentrations of electronic information aggregated into colossal databases.[4] Yet much of this same information is also consumed socially and dispersed through a user interface to hundreds, if not thousands, of peer users. In order to distinguish this relationally shared information from information in databases and the nascent concept of "big data," this essay will refer to the massive amounts of personal information shared via the user interface of social technologies as "social data." Social interaction is messy and contextual in the extreme and, like with electronic databases, social data-protection initiatives could benefit from guiding principles and a common language for policy objectives.

Yet unlike electronic databases, there are no commonly accepted principles to guide the recent explosion of voluntarily adopted practices, industry codes,

---

What Privacy Is For, 126 HARV. L. REV. 1904, 1918–19 (2013) ("Efforts to repackage pervasive surveillance as innovation—under the moniker 'Big Data'—are better understood as efforts to enshrine the methods and values of the modulated society at the heart of our system of knowledge production."); Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1889–90 (2013) ("Modern data analytics, which is also loosely referred to as data mining or 'Big Data,' can deduce extensive information about a person from these clues. In other words, little bits of innocuous data can say a lot in combination."); Tene & Polonetsky, *supra* note 1, at 242 ("For the past four decades, the tension between data innovation and informational privacy has been moderated by a set of principles broadly referred to as the Fair Information Practice Principles (FIPPs) . . . . The big data paradigm challenges some of these fundamental principles . . . .").

[4] Privacy and security expert Bruce Schneier has developed a very useful taxonomy of Social Networking Data:

> • ***Service data*** is the data you give to a social networking site in order to use it. Such data might include your legal name, your age, and your credit-card number.
> • ***Disclosed data*** is what you post on your own pages: blog entries, photographs, messages, comments, and so on.
> • ***Entrusted data*** is what you post on other people's pages. It's basically the same stuff as disclosed data, but the difference is that you don't have control over the data once you post it—another user does.
> • ***Incidental data*** is what other people post about you: a paragraph about you that someone else writes, a picture of you that someone else takes and posts. Again, it's basically the same stuff as disclosed data, but the difference is that you don't have control over it, and you didn't create it in the first place.
> • ***Behavioral data*** is data the site collects about your habits by recording what you do and who you do it with. It might include games you play, topics you write about, news articles you access (and what that says about your political leanings), and so on.
> • ***Derived data*** is data about you that is derived from all the other data. For example, if 80 percent of your friends self-identify as gay, you're likely gay yourself.

Bruce Schneier, *A Revised Taxonomy of Social Networking Data*, SCHNEIER ON SECURITY (Aug. 10, 2010, 6:51 AM), http://www.schneier.com/blog/archives/2010/08/a_taxonomy_of_s_1.html (emphasis added); *see also* Bruce Schneier, *A Taxonomy of Social Networking Data*, IEEE SECURITY & PRIVACY, July–Aug. 2010, at 88, 88.

and laws that address social data. While existing common law and statutes cover some of the problems presented by social media, the legal response to social data is becoming disjointed.[5] The purpose of this essay is to propose a set of general guiding principles for the protection of social data and to explore various ways in which these principles might be implemented—a sort of FIPPs for the front-end of social media.

To that end, this essay proposes three general principles for the protection of social data:

1) Those interacting with social data should respect an individual's expressed boundaries.
2) Those interacting with social data should respect the integrity of an individual's expressed identity.
3) Those interacting with social data should respect the integrity of an expressed social network.

These principles, which can be referred to as the *Boundary Regulation Principle*, the *Identity Integrity Principle*, and the *Network Integrity Principle*, address many of the privacy-related interests of social media users in a specific way without substantially overlapping the FIPPs and distinct, well-established areas of the law, such as intellectual property and defamation. These principles can already be seen in new and proposed rules and laws related to social data, though if they are not organized into coherent principles, courts, policymakers, and organizations risk haphazard and inconsistent rules regarding the use of social data.

Part II of this essay will explore the need for social data principles, including the conflation of threats presented by databases and other social media users, the insufficiency of the FIPPs for social data, and the seemingly haphazard onslaught of new voluntary codes and compulsory regulations aimed at protecting social data. Part III of this essay will propose the three general principles for the protection of social data, including their normative underpinning and current examples of problems that arise when the principles are not respected. Part IV will suggest various ways to implement the social data principles, including disclosure limitations, design requirements, and limitations on the use of social technologies and requests for social data. This essay concludes by noting that although principles like the social data principles are not without weaknesses, like the FIPPs, they are preferable for consistency and consensus to the haphazard promulgation of rules or the failure to articulate a common language and generally mutual goals to wrestle with the issues presented by social data.

---

[5] *See infra* Part II.B.

II. THE NEED FOR SOCIAL DATA PRINCIPLES

In his article *Saving Facebook*, James Grimmelmann rejected commercial data collection rules, which are evocative of the FIPPs, as a means to protect against what he saw as "peer-produced privacy violations." Grimmelmann stated: "[e]ven if the government left Facebook completely alone, and Facebook showed no advertisements to its users, and no other company ever had access to Facebook's data, most of the [privacy-related] problems we've seen would remain."[6] Grimmelmann adeptly articulated a primary concern in disclosing social data when he stated, "we worry about what our parents, friends, exes, and employers will see, just as much as we worry about what malevolent strangers will see."[7]

The FIPPs, which have evolved over time, have remained almost entirely focused on one technology: the database.[8] The FIPPs provide for general guiding principles to ensure concepts like limitations on data collection and use, data quality, reasonable security safeguards for data, transparency for collections of personal data, and accountability for data controllers.[9] The laws that embrace the FIPPs are also, at their core, legal responses to the threats posed by electronic databases, such as HIPAA and the Privacy Act, which deal with limitations on the collection, maintenance, use, and dissemination of personally identifiable information about individuals maintained in records systems like databases.

Grimmelmann noted that the concerns that drive commercial data collection rules like the FIPPs are not really applicable to many threats faced by social media users. Grimmelmann stated:

> [t]hese are not concerns about powerful entities looking down on the network from above; they're concerns about individuals looking at each other from ground level. Even if Facebook were perfectly ethical and completely discreet, users would still create false profiles, snoop on each other, and struggle over the bounds of the private.[10]

Social data principles are needed because the current laws, guidelines, and company policies and design strategies need a common language and policy objective to consistently capture the range of problems posed by social data. The emerging laws designed to fill that gap are increasingly disjointed and

---

[6] James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1188 (2009).

[7] *Id.*

[8] *See generally* Gellman, *supra* note 1; Bartosz M. Marcinkowski, *Privacy Paradox(es): In Search of a Transatlantic Data Protection Standard*, 74 OHIO ST. L.J. 1167 (2013).

[9] Gellman, *supra* note 1; *see also* Claudia Diaz, Omer Tene & Seda Gürses, *Hero or Villain: The Data Controller in Privacy Law and Technologies*, 74 OHIO ST. L.J. 923 (2013).

[10] Grimmelmann, *supra* note 6, at 1189.

haphazard.[11] The FIPPs are largely inapplicable to problems that arise when individuals interact with each other at the "social" level. These interactions are instead reliant upon a loose patchwork of torts, statutes, regulations, contracts, employer policies, and industry guides, which have failed to meaningfully coalesce to give the handlers and subjects of social data clear guidance and common goals.

An attempt to find common social data goals is daunting in light of the highly contextual and divergent vulnerabilities wrought by social data. But it is important in light of the resulting harm that can come from peer and outsider misuse of that data. Facebook users alone face a laundry list of harms, ranging from malicious disclosures by faithless "friends"[12] to harms resulting from well-intentioned or accidental disclosures.[13] Many employees have lost their jobs when employers access social data.[14] Others have suffered loss as the result of judgments made based on decontextualized or misinterpreted social data, such as the Canadian woman who lost her benefits for the treatment of depression due to the cheerful disposition she displayed on her Facebook profile.[15]

Many social data harms extend beyond pecuniary loss and include emotional and social harms as well. Consider Bobbi Duncan and Taylor McCormick, to whom the dangers of social data were made abundantly clear.[16] The sexual preferences of these two students at the University of Texas were inadvertently revealed to their parents when they were added to the Facebook group for Queer Chorus, a student organization.[17] Although both students were allegedly sophisticated users who attempted to obfuscate their online activity from their parents, their privacy settings were not respected by the "Groups" Facebook function, which allows Facebook users to be added to a group by a

---

[11] *See, e.g.*, Goldman, *supra* note 2.

[12] *See, e.g.*, Will Ripley, *Denver Man Fired for Complaining About Work on Facebook*, 9NEWS.COM (May 7, 2013, 10:22 PM), http://www.9news.com/news/article/334929/222/Denver-man-fired-for-complaining-about-work-on-Facebook ("'I got to a point where I put a comment on Facebook that got me fired,' [employee] said. [Employee]'s coworker reported him to their boss.").

[13] *See* Geoffrey A. Fowler, *When the Most Personal Secrets Get Outed on Facebook*, WALL ST. J., Oct. 13, 2012, http://online.wsj.com/article/SB10000872396390444165804578008740578200224.html.

[14] FACEBOOK FIRED, https://thefacebookfired.wordpress.com/ (last visited Aug. 22, 2013) (aggregating links to stories about employees fired as a result of postings made on Facebook and other social media); *see also* Daniel Solove, *Employers and Schools that Demand Account Passwords and the Future of Cloud Privacy*, CONCURRING OPINIONS (June 3, 2013, 10:51 AM), http://www.concurringopinions.com/archives/2013/06/employers-and-schools-that-demand-account-passwords-and-the-future-of-cloud-privacy.html.

[15] Bruce Watson, *Facebook Spying Costs Canadian Woman Her Health Benefits*, DAILYFINANCE (Nov. 23, 2009, 5:30 PM), http://www.dailyfinance.com/2009/11/23/facebook-spying-costs-canadian-woman-her-health-benefits/.

[16] Fowler, *supra* note 13.

[17] *Id.*

friend without their approval.[18] The creator of the choir's Facebook group did not realize that adding users to the group automatically reported the users' new membership to their Facebook "friends."[19]

Such accidental disclosures—as well as more malicious ones—highlight the need for more focused design-based solutions to privacy as well as organizational policies that better articulate the boundaries of disclosure, such as whether the choir's Facebook page should have been set to "private" instead of "public," or whether Facebook's software should better incorporate the expressed wishes of its users as part of the "privacy by design" initiative.[20] Established information practice principles could guide these decisions.

But the FIPPs are a poor fit to help Ms. Duncan, Mr. McCormick, and the countless other Internet users who have experienced the harmful consequences of others disclosing and interacting with social data. This Part will briefly explore the various threats posed by social data, as well as the insufficiency of established laws to respond to those threats and the haphazard nature of the emerging social data protections that seek to fill the void.

A. *The Threat of Peers and Outsiders*

Social media produce data that exists both on the "front end" and "back end" of the technology.[21] One piece of information, such as a shared photo or status update, can simultaneously be presented via a user interface as social data as well as aggregated into a database for commercial purposes. Thus, when discussing the threats to personal information disclosed on social media, it is important to distinguish between data contexts and properly situate the potential harm at issue. This can be difficult given the increased media attention to the

---

[18] *Id.*

[19] *Id.*

[20] *See* ANN CAVOUKIAN, PRIVACY BY DESIGN 1 (2009), *available at* http://www.ipc.on.ca/images/Resources/privacybydesign.pdf; *see also* FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS, at vii (2012), *available at* http://ftc.gov/os/2012/03/120326privacyreport.pdf; Article 29 Data Protection Working Party & Working Party on Police and Justice, The Future of Privacy, at 3 (Dec. 1, 2009), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf; Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31; Travis D. Breaux & Annie I. Antón, *Analyzing Regulatory Rules for Privacy and Security Requirements*, 34 IEEE TRANSACTIONS ON SOFTWARE ENGINEERING 5, 10 (2008); Ira S. Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L.J. 1409, 1421 (2011) ("Privacy by design is an amorphous concept."); Ira S. Rubinstein & Nathaniel Good, *Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents* 4 (N.Y. Univ. Sch. of Law, Working Paper No. 12-43, 2012), *available at* https://www.privacyassociation.org/media/pdf/events_and_programs/Privacy%20by%20Design-A%20Counterfactual%20Analysis.pdf.

[21] *See* Schneier, *supra* note 4.

topic of privacy on the Internet that tends to conflate social media harms. For example, the *Wall Street Journal* has produced an impressive collection of stories about digital privacy under the title *What They Know*.[22] But it is not clear, at least initially, whether "they" refers to websites, third-party advertising networks, governments, employers, other users, or all of the above.

One helpful metaphor for distinguishing the database privacy threat from the user interface privacy threat is the stage.[23] Information that is collected by websites and applications and stored in databases exists "backstage." This data collection and use, which is typically not visible to users, is what is most commonly referenced when referring to "data protection."[24] Backstage data underlies such concepts as "digital dossiers"[25] and "the database of ruin,"[26] and is the aim of most privacy-related statutes and the FIPPs.[27]

Meanwhile social data is best viewed as existing on the "front stage," in the sense that it is visible to other users via the user interface of social technologies. While the danger created by electronic databases lies in the concentration of the information, social data is dangerous due to the high number of potential harmful actors and the amorphous, semi-private nature of information disclosed via social technologies. Airi Lampinen observed, "[c]onventional privacy and computer security studies focus on threats and risks created by faceless third parties. In social media, end-user privacy concerns are more than before related to real second parties[—]people who are known also offline and who are anything but faceless."[28]

Some of the most prominent examples of technologies that aid in the creation of social data are social network sites, but the concept also extends to

---

[22] *What They Know*, WALL ST. J., http://online.wsj.com/public/page/what-they-know-digital-privacy.html (last visited Jan. 29, 2013).

[23] *See* ERVING GOFFMAN, THE PRESENTATION OF SELF IN EVERYDAY LIFE 22–30 (1973). For Goffman, "backstage" was a place where one could be more free to be one's self without as many prying eyes. *Id.* at 111–40. The back stage identified in this Article refers to limited visibility. Many website users can theoretically see "front stage" data, while only an organization and authorized intermediaries have initial lawful access to "backstage" data.

[24] *See, e.g.*, Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 357 ("Although most industrialized nations have comprehensive data protection laws, the United States has maintained a sectoral approach where certain industries are covered and others are not. In particular, emerging companies known as 'commercial data brokers' have frequently slipped through the cracks of U.S. privacy law.").

[25] DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 1 (2004); Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1140 (2002).

[26] Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1748 (2010).

[27] *See* Gellman, *supra* note 1, at 2.

[28] Airi Lampinen, *Practices of Balancing Privacy and Publicness in Social Network Services*, *in* PROCEEDINGS OF THE 16TH ACM INTERNATIONAL CONFERENCE ON SUPPORTING GROUP WORK 343, 343 (2010), *available at* http://delivery.acm.org/10.1145/1890000/1880142/p343-lampinen.pdf.

other technologies such as blogs, bulletin boards, games, and any other digital medium used to socialize within an online community. Since the focus of social data is on context, actors, and information, difficult and potentially artificial distinctions between the different kinds of social technologies are largely unnecessary.

Thinking of social data and database information as existing on a front stage and back stage, respectively, is helpful when comparing the two—a necessary step in developing distinct principles. Social data is similar to "big data," if in no other way, in sheer magnitude. Yet instead of more data being aggregated into one centralized location, social data's largeness comes from the enormous number of disclosers and recipients, each contributing a relatively small amount of data. According to the Pew Internet & American Life Project, as of May 2013, seventy-two percent of online adults use social networking sites.[29] As of August 2012, forty-six percent of adult internet users post original photos or videos online that they themselves have created.[30] Forty-one percent of adult internet users take photos or videos that they have found online and repost them on sites designed for sharing images with many people.[31]

According to other sources, in one day on the Internet:

> Enough information is consumed to fill 168 million DVDs. 294 billion emails are sent. 2 million blog posts are written (enough posts to fill TIME magazine for 770 million years). 172 million people visit Facebook. 40 million visit Twitter. 22 million visit LinkedIn. 20 million visit Google+. 17 million visit Pinterest. 4.7 billion minutes are spent on Facebook. 532 million statuses are updated. 250 million photos are uploaded. . . . 864,000 hours of video are uploaded to YouTube. More than 35 million apps are downloaded. More iPhones are sold than people are born.[32]

There are a number of important differences between front stage and backstage data. Unlike online information that is disclosed and used in the commercial, financial, and healthcare context, social data is often disseminated online for enjoyment or emotional support, to create and strengthen relationships and communities, or for simple self-promotion.[33] Although

---

[29] JOANNA BRENNER & AARON SMITH, PEW RESEARCH CTR., 72% OF ONLINE ADULTS ARE SOCIAL NETWORKING SITE USERS 2 (2013), *available at* http://pewinternet.org/~/media//Files/Reports/2013/PIP_Social_networking_sites_update.pdf.

[30] LEE RAINIE ET AL., PEW RESEARCH CTR, PHOTOS AND VIDEOS AS SOCIAL CURRENCY ONLINE 2 (2012), *available at* http://pewinternet.org/~/media//Files/Reports/2012/PIP_OnlineLifeinPictures_PDF.pdf.

[31] *Id.*

[32] Cara Pring, *100 Social Media, Mobile and Internet Statistics for 2012 (March)*, SOCIAL SKINNY (Mar. 21, 2012), http://thesocialskinny.com/100-social-media-mobile-and-internet-statistics-for-2012/.

[33] *See, e.g.*, Susan Waters & James Ackerman, *Exploring Privacy Management on Facebook: Motivations and Perceived Consequences of Voluntary Disclosure*, 17 J. COMPUTER-MEDIATED COMM. 101, 105 (2011).

socially shared information has always left disclosers of information vulnerable to privacy harms, until recently this threat was less than pervasive. Before entrenchment of the social web, most social interaction was ephemeral, on paper, or one-to-few. Facebook, YouTube, and the host of social media have overseen an explosion of social data, which is increasingly absorbing the web and complicating our online existence.

So who exactly are threats to social data? Maritza Johnson, Serge Egelman, and Steven Bellovin have identified the most unwanted audiences viewing social media disclosures as "future employers, supervisors, family members, peers and subordinates," and general "social threats" in addition to "organizational threats" related to the collection and use of data from social network sites.[34]

These relationships are different in important ways from users' relationships with the social media company itself. The relationship between social media users and the website itself regarding privacy is ostensibly governed by, among other things, the website's privacy policy.[35] However, the relationship between users and their peers is governed by a much more complex and unstable set of norms, shared assumptions, informal terms, and a host of other signals and cultural contexts.[36] Consider the two major kinds of individuals who have or want access to social data—insiders and outsiders—and the related user vulnerabilities.

1. *Insiders*

The most proximate threats to social data are "insiders"—those selected to be recipients of, or at least have access to, online disclosures. Our "friends," "followers," and other networked connections are all in positions to misuse social data immediately upon disclosure. Members of online social networks have had information disclosed, presumably by insiders, to outsiders in harmful

---

[34] Maritza Johnson et al., *Facebook and Privacy: It's Complicated*, *in* PROCEEDINGS OF THE 8TH SYMPOSIUM ON USABLE PRIVACY AND SECURITY, at 2.1 (2012), *available at* http://cups.cs.cmu.edu/soups/2012/proceedings/a9_Johnson.pdf (including in the "threats" category people purposefully posting content to harm the individual and a general concern over a lack of control over the actions of other users).

[35] *See* Woodrow Hartzog, *Website Design as Contract*, 60 AM. U. L. REV. 1635, 1635 (2011); Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control over Personal Information?*, 111 PENN ST. L. REV. 587, 588 (2007).

[36] *See* Woodrow Hartzog, *Reviving Implied Confidentiality*, 89 IND. L.J. (forthcoming 2014); Woodrow Hartzog & Frederic Stutzman, *The Case for Online Obscurity*, 101 CALIF. L. REV. 1, 8 (2013); Woodrow Hartzog & Frederic Stutzman, *Obscurity by Design*, 88 WASH. L. REV. 385, 401 (2013); Woodrow Hartzog, *The Problems and Promise with Terms of Use as the Chaperone of the Social Web*, CONCURRING OPINIONS (June 11, 2013, 1:09 AM), http://www.concurringopinions.com/archives/2013/06/the-problems-and-promise-with-terms-of-use-as-the-chaperone-of-the-social-web.html.

ways.[37] In one instance, Facebook asked its users to report whether the user's "friends" were using their real name, a requirement under the website's terms of use.[38]

In some instances, even insiders who have been explicitly granted access to social data are not the desired recipients. At first blush, it seems nonsensical to suggest that users would like to hide self-disclosed information from those who have been explicitly authorized by the user to view this same information. But social interaction online is not so simple. Recall the University of Texas students whose sexuality was revealed to their parents via their "friendship" on Facebook.[39] Also consider Facebook's new "Graph Search" feature.[40] Users forget or do not always realize the true extent of their potential audience when they post.[41] Similar concerns are raised by the automatic, accidental, or forced sharing of browsing and reading habits through "frictionless sharing."[42]

---

[37] *See, e.g.*, FACEBOOK FIRED, *supra* note 14 (detailing reports of many social media users disciplined for their posts, many of which were reported by the user's social network connections); Geoffrey Fowler, *Three Facebook Privacy Loopholes*, WALL ST. J. BLOG (Oct. 12, 2012, 10:33 PM), http://blogs.wsj.com/digits/2012/10/12/three-facebook-privacy-loopholes/?mod=WSJBlog; Will Oremus, *Could Your Crummy Klout Score Keep You from Getting a Job?*, SLATE FUTURE TENSE (Oct. 3, 2012, 12:35 PM), http://www.slate.com/blogs/future_tense/2012/10/03/online_privacy_can_employers_use_klout_scores_facebook_profiles_to_screen_applicants_.html ("There are also plen[t]y of instances of workers being fired for Facebook posts even if their employers don't have access to their accounts.").

[38] Carl Franzen, *Facebook Surveying Users About Their Friends' Fake Usernames*, TALKING POINTS MEMO IDEALAB (Sept. 20, 2012, 6:12 PM), http://idealab.talkingpointsmemo.com/2012/09/facebook-confirms-its-surveying-users-about-their-friends-fake-usernames.php.

[39] *See* Fowler, *supra* note 13.

[40] Woodrow Hartzog & Evan Selinger, *Obscurity: A Better Way To Think About Your Data than "Privacy,"* ATLANTIC (Jan. 17, 2013, 12:55 PM), http://www.theatlantic.com/technology/archive/2013/01/obscurity-a-better-way-to-think-about-your-data-than-privacy/267283/.

[41] Yang Wang et al., *From Facebook Regrets to Facebook Privacy Nudges*, 74 OHIO ST. L.J. 1307, 1313–18 (2013). This fact is often evident when employees are fired for complaining about their jobs to their Facebook "friends," at least one of whom was the employee's boss.

[42] According to Neil Richards, "[u]nder a regime of 'frictionless sharing,' we don't need to choose to share our activities online. Instead, everything we read or watch automatically gets uploaded to our Facebook or Twitter feed." Neil M. Richards, *The Perils of Social Reading*, 101 GEO. L.J. 689, 691 (2013); *see also id.* at 713 ("There are just three problems with making frictionless sharing of reader records our default: [f]rictionless sharing isn't frictionless, it isn't really sharing, and it's corrosive of intellectual privacy and intellectual freedom."); William McGeveran, *The Law of Friction*, 2013 U. CHI. LEGAL F. (forthcoming 2013); Somini Sengupta, *Private Posts on Facebook Revealed*, N.Y. TIMES BITS (Jan. 18, 2013, 6:52 PM), http://bits.blogs.nytimes.com/2013/01/18/private-posts-on-facebook-revealed/.

2. *Outsiders*

Outsiders, conceptualized here as those without access to protected social data, can serve as threats by both seeking access to social data and disclosing one's personal information online in social contexts in which that person is not a part. One of the most significant drivers of social data protections is the threat of outsiders seeking social data that is protected or otherwise hidden.[43] There have been numerous instances of employers asking for social media passwords or access to social media.[44] School administrators are often tempted to monitor social media usage.[45] Police officers[46] and other entities have an interest in accessing social data.[47] Facebook's targeted ad campaign can potentially be used to determine whether some users are gay.[48]

---

[43] Solove, *supra* note 14 ("I thought that the practice of demanding passwords was so outrageous that it couldn't be very common . . . . But . . . the practice is much more prevalent than I had imagined, and it is an issue that has very important implications as we move more of our personal data to the Cloud.").

[44] *See, e.g.*, Joanna Stern, *Demanding Facebook Passwords May Break Law, Say Senators*, ABC NEWS (Mar. 26, 2012), http://abcnews.go.com/Technology/facebook-passwords-employers-schools-demand-access-facebook-senators/print?id=16005565.

[45] *See, e.g.*, John Browning, *Universities Monitoring Social Media Accounts of Student-Athletes: A Recipe for Disaster*, 75 TEX. BAR J. 840, 840 (2012), *available at* http://www.texasbar.com/AM/Template.cfm?Section=Texas_Bar_Journal&Template=/CM/ContentDisplay.cfm&ContentID=20538; Sandra Engelland, *Keller District Officials Look to Extra Security, Monitoring Social Media To Prevent Pranks*, KELLER CITIZEN (May 28, 2013), http://www.star-telegram.com/2013/05/28/4888860/keller-district-officials-look.html; Michael Hartwell, *Schools Monitor Students' Posts on Facebook, Twitter*, SENTINEL & ENTERPRISE (Jan. 14, 2013, 7:01 AM), http://www.sentinelandenterprise.com/topstory/ci_22369565/schools-monitor-students-posts-facebook-twitter.

[46] *See, e.g.*, Benny Evangelista, *Social Media Monitored More by Law Enforcement*, SFGATE (Aug. 13, 2011, 4:00 AM), http://www.sfgate.com/business/article/Social-media-monitored-more-by-law-enforcement-2335017.php; Priya Kumar, *Law Enforcement and Mining Social Media: Where's the Oversight?*, INTERNET MONITOR (July 1, 2013), https://blogs.law.harvard.edu/internetmonitor/2013/07/01/law-enforcement-and-mining-social-media-wheres-the-oversight/; Paul Wagenseil, *British Cops Admit They Monitor Facebook, Twitter*, TECHNEWSDAILY (June 27, 2013, 5:42 PM), http://www.technewsdaily.com/18448-socmint-police-monitoring.html.

[47] *See, e.g.*, Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST, June 6, 2013, http://articles.washingtonpost.com/2013-06-06/news/39784046_1_prism-nsa-u-s-servers (discussing leaked documents implying that the National Security Agency had direct access to Facebook servers). *But see* Ted Ullyot, *Facebook Releases Data, Including All National Security Requests*, FACEBOOK NEWSROOM (June 14, 2013), http://newsroom.fb.com/News/636/Facebook-Releases-Data-Including-All-National-Security-Requests (denying allegations of direct server access, but disclosing that U.S. government entities requested Facebook data between 9,000 and 10,000 times in the six months prior to December 31, 2012).

[48] Adrian Chen, *How Facebook's Targeted Ads Revealed One User's Sexuality*, GAWKER (Oct. 23, 2010, 12:57 PM), http://gawker.com/5671582/how-facebooks-targeted-ads-revealed-one-users-sexuality.

Outsiders might also post information on the social web. For example, a number of healthcare workers have been disciplined for publishing their patients' sensitive health-related information on social media.[49] Police officers and emergency responders have been disciplined for disclosing personal details of those with whom they interact.[50] Numerous websites and conversation threads expose or shame customers and other people who violate social norms such as tipping[51] and proper dating etiquette.[52] It should be noted, however, that problems of outsiders posting personal information on the Internet are broader than the narrower focus of insiders disclosing, and outsiders seeking, social data. As such, these problems are beyond the scope of this Article.

B. *The Haphazard Emerging Protection of Social Data*

Although database protections have little effect on social data, the law does provide some remedy for social data harms. But these remedies are either too narrow in scope or too burdensome to be effective for most social data problems. For example, the privacy torts ostensibly protect against the public disclosure of private facts, intrusion upon seclusion, appropriation of one's name or likeness, and depiction of an individual in a false light—all potential

---

[49] *E.g.*, *CNA Put Nasty Photo of Patient on Facebook, Officials Say*, RTV6 (July 21, 2011), http://www.theindychannel.com/news/cna-put-nasty-photo-of-patient-on-facebook-officials-say; Molly Hennessy-Fiske, *When Facebook Goes to the Hospital, Patients May Suffer*, L.A. TIMES, Aug. 8, 2010, http://articles.latimes.com/2010/aug/08/local/la-me-facebook-20100809.

[50] J. David Goodman & Wendy Ruderman, *Police Dept. Sets Rules for Officers' Use of Social Media*, N.Y. TIMES, Mar. 28, 2013, http://www.nytimes.com/2013/03/29/nyregion/new-york-police-dept-issues-guidelines-for-social-media.html?_r=0 ("Last year, one Brooklyn precinct commander was criticized for posting photographs of men about to be released from custody to a Twitter account maintained by the precinct."); Candice M. Giove & Brad Hamilton, *FDNY EMS Workers Post Gory, Private Photos of Patients Online*, N.Y. POST, Mar. 31, 2013, http://nypost.com/2013/03/31/fdny-ems-workers-post-gory-private-photos-of-patients-online/ ("[S]ome first responders can't resist snapping shots of people they're supposed to be helping.").

[51] John Del Signore, *Are You Named on This Website Outing Bad Tippers?*, GOTHAMIST (Apr. 29, 2011, 3:28 PM), http://gothamist.com/2011/04/29/are_you_named_on_this_website_outin.php; LOUSYTIPPERS.COM, http://www.lousytippers.com/ (last visited July 2, 2013); *see also* Neetzan Zimmerman, *Pastor Who Left Sanctimonious Tip Gets Waitress Fired from Applebee's, Claims Her Reputation Was Ruined*, GAWKER (Jan. 31, 2013, 1:03 PM), http://gawker.com/5980558/pastor-who-left-sanctimonious-tip-gets-waitress-fired-from-applebees-claims-her-reputation-was-ruined.

[52] *See* Anna North, *"Yelp for Guys" Founder Hopes It Makes Men Better*, BUZZFEED (Feb. 6, 2013, 3:08 PM), http://www.buzzfeed.com/annanorth/yelp-for-guys-founder-hopes-it-makes-men-better ("Lulu lets women (and only women) create 'reviews' of men they know."); REPORT YOUR EX, http://reportyourex.com/ (last visited July 2, 2013); *see also* DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 50–53 (2007).

harms enabled by social data.[53] Yet the First Amendment's broad exclusions for "newsworthy" and "public" information mean that the torts are not very effective online.[54]

In light of this failure, the government and private organizations might seek to protect users of social technologies. State legislatures have sought to limit employer and educator access to social data.[55] Organizations and entire industries have begun to promulgate social media guidelines.[56] But what should guide them other than an instinctual sense that not all information disclosed via social media should be free for everyone to use? There is no common guidance for the emerging peer-focused privacy protections.

For example, at the time this Article was written at least eleven states have planned to consider whether to regulate employer and school administrator access to the personal social media accounts of employees, job applicants, and students.[57] Maryland, Illinois, Delaware, California, New Jersey, Michigan, and Utah have already enacted measures that limit employer or school administrator access to social media accounts.[58] Some critics contend that such laws vastly

---

[53] *See* RESTATEMENT (SECOND) OF TORTS §§ 652A–652E (1977).

[54] *See* Roberts v. CareFlite, No. 02–12–00105–CV, 2012 WL 4662962, at *4 (Tex. Ct. App. Oct. 4, 2012); Neil M. Richards, *The Limits of Tort Privacy*, 9 J. TELECOMM. & HIGH TECH. L. 357, 361 (2011) ("[T]he First Amendment should trump disclosure privacy in all but a narrow category of cases."); Daniel J. Solove, *The Slow Demise of Defamation and the Privacy Torts*, HUFFINGTON POST (Oct. 11, 2010, 4:52 PM), http://www.huffingtonpost.com/daniel-j-solove/the-slow-demise-of-defama_b_758570.html.

[55] *See, e.g.*, David L. Hudson, Jr., *Site Unseen: Schools, Bosses Barred from Eyeing Students', Workers' Social Media*, ABA JOURNAL (Nov. 1, 2012, 3:10 AM), http://www.abajournal.com/magazine/article/site_unseen_schools_bosses_barred_from_eyeing_students_workers_social_media; Solove, *supra* note 14.

[56] *See, e.g.*, Angela Haggerty, *CPS Publishes Social Media Crime Guidelines for Prosecutors as Police Are Deluged with Complaints*, DRUM (June 20, 2013, 12:07 PM), http://www.thedrum.com/news/2013/06/20/cps-publishes-social-media-crime-guidelines-prosecutors-police-are-deluged#OrHeOT1pVztIZsuW.99; Theresa Lee & Brian Wong, *Safe Tweeting: SEC Provides Guidance on Social Media and Regulation FD Compliance*, JDSUPRA L. NEWS (Apr. 11, 2013), http://www.jdsupra.com/legalnews/safe-tweeting-sec-provides-guidance-on-70644/; Sarah Peters, *Lopatcong Township Council Adopts Social Media Policies Prior to Launching Facebook, Twitter Accounts*, LEHIGHVALLEYLIVE.COM (June 14, 2013, 5:30 AM), http://www.lehighvalleylive.com/phillipsburg/index.ssf/2013/06/lopatcong_township_council_ado.html; David Sims, *Social Media Policies Present Challenges to Business*, IMT (June 18, 2013), http://news.thomasnet.com/IMT/2013/06/18/social-media-policies-present-challenges-to-business/.

[57] ABA Section of Labor & Emp't Law Emp't Rights & Responsibilities Comm., A Survey of State Laws Relating to Social Networking Privacy and Other Recent Developments in Workplace Privacy Law 3–4, 7, 9–11, 13–16 (presented at the Midwinter Meeting, Mar. 19–23, 2013), *available at* http://www.americanbar.org/content/dam/aba/events/labor_law/2013/03/employment_rightsresponsibilitiescommitteemidwintermeeting/26_developments.authcheckdam.pdf.

[58] MD. CODE ANN., LAB. & EMPL. § 3-712 (LexisNexis Supp. 2012); 820 ILL. COMP. STAT. 55/10 (2012); DEL. CODE ANN. tit. 14, §§ 8101–8105 (Supp. 2012); CAL. EDUC. CODE §§ 99120–99122 (West Supp. 2013); CAL. LAB. CODE § 980 (West Supp. 2013); N.J. STAT.

and unnecessarily expand previously existing privacy protections in the United States in addition to creating an inconsistent patchwork of statutes.[59]

Professor Eric Goldman has noted two problems with California's attempt to protect social data from employers: 1) the law is too broad because "social media" is too difficult to define; and 2) the law falsely assumed a bright-line dichotomy between "personal" and "non-personal" accounts.[60] Phillip L. Gordon, Amber M. Spataro, and William J. Simmons noted that:

> [t]hese laws, however, do not follow a model with identical or nearly identical terms. Instead, they create a complex patchwork that makes it virtually impossible for a multi-state employer to establish a uniform policy: [e]ach state uses its own key terms (some of which are defined, some of which are not); [e]ach state defines its own scope of coverage (some as narrow as prohibiting only seeking login information from applicants, some as broad as prohibiting employers from requiring employees to disclose any internet content to their employers); and [e]ach state defines its own remedial scheme (some silent on remedies, some providing for a private right of action, and some requiring administrative enforcement).[61]

The inconsistencies between these laws make clear the need to articulate a set of commonly held values to guide policy and self-regulatory efforts.

III. PRINCIPLES FOR THE PROTECTION OF SOCIAL DATA

Accepted principles could provide some consistency in regulatory, self-regulatory, and design efforts. Legislators, policymakers, courts, companies, and advocates need a common language to better articulate and properly constrain unique rules or restrictions for social data, as well as to better locate

---

ANN. §§ 18A:3-29 to 3-32 (West Supp. 2013); MICH. COMP. LAWS §§ 37.273–37.275 (Supp. 2013); UTAH CODE ANN. § 34-48-201 (LexisNexis Supp. 2013).

[59] *See, e.g.*, PHILLIP L. GORDON ET AL., SOCIAL MEDIA PASSWORD PROTECTION AND PRIVACY—THE PATCHWORK OF STATE LAWS AND HOW IT AFFECTS EMPLOYERS 5 (2013), *available at* http://www.littler.com/files/press/pdf/LittlerReportSocialMediaPasswordProtectionaAndPrivacyThePatchworkOfStateLawsAndHowItAffectsEmployers.pdf ("These laws, however, do not follow a model with identical or nearly identical terms. Instead, they create a complex patchwork that makes it virtually impossible for a multi-state employer to establish a uniform policy.").

[60] Goldman, *supra* note 2; *see also* Venkat Balasubramani, *Recap of Washington State's Employer Social Media Password Bill*, ERIC GOLDMAN TECH. & MARKETING L. BLOG (May 3, 2013, 10:49 AM), http://blog.ericgoldman.org/archives/2013/05/recap_of_washin.htm (predicting that a new bill will cause more problems than it solves); Venkat Balasubramani, *Washington State's Proposed Employer Social Media Law: The Legislature Should Take a Cautious Approach—SB 5211*, ERIC GOLDMAN TECH. & MARKETING L. BLOG (Feb. 9, 2013, 8:25 AM), http://blog.ericgoldman.org/archives/2013/02/washingtons_pro.htm (criticizing new law for lack of clarity in defining social media).

[61] GORDON ET AL., *supra* note 59, at 5.

existing, perhaps more broadly applicable rules that might also apply to social data.

A few have already attempted to create guidelines for social data under different names, most notably the *Social Network Constitution*,[62] *Social Network Users Bill of Rights*,[63] and *A Bill of Privacy Rights for Social Network Users*.[64] These are either over-inclusive for the purpose of social data guidance because they focus on databases and commercial use of information in addition to social harms, or are not quite specific enough to use as a true guide in crafting rules for social data.

A truly effective set of principles would unite social data issues to serve as a complementary addition to, rather than replacement of, the FIPPs. The principles must be flexible enough to apply across many different social contexts and reach the behavior of both insiders and outsiders, while also providing enough substance to serve as a meaningful lodestar for legislators, judges, administrators, companies, designers, and law enforcement officials. In order to be this flexible, the principles should not specifically address organizational-specific concerns, such as serving especially vulnerable populations or hosting abnormally sensitive information, which might require more robust and specific regulations.[65]

So what is important to users on the social web? Culling from existing laws, relevant literature, and current disputes, it appears that the three most important privacy-related concepts are boundaries, identity, and network integrity. Using the language of mandated principles similar to the FIPPs, this essay proposes that these three concepts can serve as the basis of the social data principles.

---

[62] Lori Andrews, *The Social Network Constitution*, SOCIAL NETWORK CONSTITUTION, http://www.socialnetworkconstitution.com/the-social-network-constitution.html (last visited June 12, 2013).

[63] Alison Diana, *Social Networking Bill of Rights Released*, INFO. WEEK SECURITY (June 23, 2010, 11:51 AM), http://www.informationweek.com/security/privacy/social-networking-bill-of-rights-release/225701171.

[64] Kurt Opsahl, *A Bill of Privacy Rights for Social Network Users*, ELECTRONIC FRONTIER FOUND. (May 19, 2010), https://www.eff.org/deeplinks/2010/05/bill-privacy-rights-social-network-users.

[65] For an example of sector specific guidelines, the SEC recently released its 2013 guidance on the use of social media by publicly traded corporations under Regulation FD. *See* SEC. & EXCH. COMM'N, REPORT OF INVESTIGATION PURSUANT TO SECTION 21(a) OF THE SECURITIES EXCHANGE ACT OF 1934: NETFLIX, INC., AND REED HASTINGS, EXCHANGE ACT RELEASE NO. 69279, at 2 (Apr. 2, 2013), *available at* http://www.sec.gov/litigation/invest report/34-69279.pdf; *see also* Mark T. Plitcha et al., *SEC's Netflix Report Confirms Ability To Use Social Media for Reg. FD Disclosures but Cites Risks*, MARTINDALE (Apr. 9, 2013), http://www.martindale.com/corporate-law/article_Foley-Lardner-LLP_1748682.htm (giving a background and summary of SEC guidance).

A. *Those Interacting with Social Data Should Respect an Individual's Expressed Boundaries*

One of the most important and relevant conceptualizations of privacy in social interactions is social psychologist Irwin Altman's theory of privacy as a process of boundary regulation.[66] Specifically, Altman conceives of privacy as "selective control of access to the self" and draws heavily from contextual settings.[67] Altman theorizes that privacy has five properties:

> 1) Privacy involves a mental process whereby we change how open or closed we are in response to changes in our internal states and external conditions.
> 2) There is a difference between actual and desired levels of privacy.
> 3) Privacy is a non-monotonic function, with an optimal level of privacy and the possibility of too much privacy.
> 4) Privacy is bi-directional, involving inputs from others (e.g. noise) and outputs to others (e.g. oral communications).
> 5) Privacy applies at the individual and group levels of analysis.[68]

The model specified by Altman envisions privacy as an ongoing, discursive, optimizing process.[69] As individuals move through contexts, they perceive stimuli (noise, light, communication). Based on the individual's goals in the context, boundaries of communication are opened (e.g. disclosing to a new acquaintance) or closed (e.g. withdrawing from a noisy cocktail party) in relation to the stimuli. Because privacy is a vague and evolving concept, Altman specifies that individuals continually manage their boundaries in order to optimize their privacy or disclosure goals.[70]

Boundary regulation theory is an ideal and developed theory of privacy for social data because it is built around the need for Internet users to disclose personal information to some, but not all. Two theories influenced by Altman's theory of privacy regulation are Sandra Petronio's Communications Privacy

---

[66] IRWIN ALTMAN, THE ENVIRONMENT AND SOCIAL BEHAVIOR: PRIVACY, PERSONAL SPACE, TERRITORY, CROWDING 27 (1975); Woodrow Hartzog, *The Privacy Box: A Software Proposal*, 14 FIRST MONDAY (Nov. 2, 2009), http://firstmonday.org/ojs/index.php/fm/article/view/2682/2361.

[67] ALTMAN, *supra* note 66, at 18; *see also* HELEN NISSENBAUM, PRIVACY IN CONTEXT 186 (2010).

[68] Hartzog, *supra* note 66 (citing ALTMAN, *supra* note 66); *see also* Stephen T. Margulis, *On the Status and Contribution of Westin's and Altman's Theories of Privacy*, 59 J. SOC. ISSUES 411, 412 (2003).

[69] *See* Fred Stutzman & Woodrow Hartzog, *Boundary Regulation in Social Media*, *in* PROCEEDINGS OF THE ACM 2012 CONFERENCE ON COMPUTER SUPPORTED COOPERATIVE WORK 769, 771 (2012), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1566904.

[70] *Id.*

Management Theory[71] and Derlega and Chaikin's Dual Boundary Concept.[72] These theories focus on the communication between the provider and recipient of information, exploring the process by which provider and recipient of information negotiate the boundaries of the disclosure. Leysia Palen and Paul Dourish apply Altman's privacy regulation theory to social media environments, concluding that "privacy management is a dynamic response to circumstance rather than a static enforcement of rules; that it is defined by a set of tensions between competing needs; and that technology can have many impacts, by way of disrupting boundaries, spanning them, establishing new ones, etc."[73] The management of privacy in social media requires an ongoing awareness of both the social context and the ever-changing affordances of the sites.

Boundaries are necessary for effective socialization both online and offline. Boundaries that are too broad lead to social crowding and chilling effects, whereas boundaries that are too narrow can lead to isolation. Wisniewski et al. note that in the physical world, "crime, juvenile delinquency, homicide, and civil strife have all been related to social crowding and high population density."[74] In other research the authors note that "[b]oundaries are important because they help us define self, give us protection (physically and emotionally), help us manage our personal resources, and forge deeper relationships."[75] Given the importance of personal boundaries and the limited ability of people to control information post-disclosure, social data principles should seek to minimize the intentional violation of boundaries.[76]

Many boundaries are virtually impossible to express or recognize, and, as such, should not be a primary focus of those seeking to respect boundary regulation. Only those boundaries that are or should be recognized by the social data recipient should guide these principles. Social data boundaries can be established implicitly and explicitly. Implicit boundaries may be constructed

---

[71] *See* SANDRA PETRONIO, BOUNDARIES OF PRIVACY, at xvii (2002).

[72] *See generally* Valerian J. Derlega & Alan L. Chaikin, *Privacy and Self-Disclosure in Social Relationships*, 33 J. SOC. ISSUES 102 (1977).

[73] Leysia Palen & Paul Dourish, *Unpacking "Privacy" for a Networked World*, *in* PROCEEDINGS OF THE ACM SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 129, 135 (2003), *available at* http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=0064B56D05CEF59AA66EE48001C204C8?doi=10.1.1.117.7183&rep=rep1&type=pdf (discussing the tensions between privacy and publicity).

[74] Pamela J. Wisniewski, Heather Richter Lipford & David C. Wilson, *Fighting for My Space: Coping Mechanisms for SNS Boundary Regulation*, *in* PROCEEDINGS OF THE SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 609, 610 (2012), *available at* dl.acm.org/ft_gateway.cfm?ftid=1216916&id=2207761.

[75] Pamela Karr-Wisniewski et al., *A New Social Order: Mechanisms for Social Network Site Boundary Regulation*, *in* PROCEEDINGS OF THE AMCIS 1 (2011), *available at* http://aisel.aisnet.org/amcis2011_submissions/101.

[76] Lampinen, *supra* note 28, at 343 ("As boyd has stated, in a social network site, privacy is a function of one's disclosures, and the disclosures about one's self by others in the site. No one can fully control the content concerning him/herself that is being shared.").

through action, such as the creation of speech codes that signify in-group memberships. Alternately, explicit boundaries may be established with privacy settings, friending practices, or by obfuscating identifiers.[77] There seem to be three distinct boundaries relevant for those interacting with social data: relational, contextual, and temporal. These boundaries can be violated with respect to social data by posting the information of others on social media as well as sharing another's self-disclosed social data with unauthorized individuals.

1. *Rational Boundaries*

One of the most fundamental boundaries set by social data users is within relationships. When users disclose information to someone, they often do not want that person to tell anyone else.[78] Relational boundaries are the foundation for numerous privacy laws, such as HIPAA,[79] as well as the doctrine of confidentiality, which is one of the oldest and most fundamental concepts within privacy law.[80]

There are numerous relatively recent examples of people who seek or are exposed to social data failing to respect relational boundaries. One of the most obvious examples is the odious practice of non-consensual pornography, sometimes called "revenge porn," which is sometimes shared via social technologies.[81] In many contexts, this would seem to be a brazen breach of confidentiality and, consequently, a violation of social data boundaries.[82]

Other kinds of boundaries, such as those established via technology, are also routinely violated. For example, countless employees have been fired after content protected by privacy settings has been disclosed by indiscreet "friends."[83]

---

[77] *See* Stutzman & Hartzog, *supra* note 69, at 773.

[78] NISSENBAUM, *supra* note 67, at 84–88; Lauren Gelman, *Privacy, Free Speech, and "Blurry-Edged" Social Networks*, 50 B.C. L. REV. 1315, 1317 (2009); *see also* Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 919–20 (2005).

[79] *See* Woodrow Hartzog, *Chain-Link Confidentiality*, 46 GA. L. REV. 657, 676–79 (2012); Peter A. Winn, *Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law*, 33 RUTGERS L.J. 617, 619 (2002).

[80] *See, e.g.*, Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 123–26 (2007); Hartzog, *Reviving Implied Confidentiality*, *supra* note 36.

[81] *See, e.g.*, Hartzog, *Reviving Implied Confidentiality*, *supra* note 36; Woodrow Hartzog, *How To Fight Revenge Porn*, ATLANTIC (May 10, 2013, 1:42 PM), http://www.theatlantic.com/technology/archive/2013/05/how-to-fight-revenge-porn/275759/; Anita Ramasastry, *Revenge Porn Returns, with Home Addresses: Why the Site Is Legal and What Legislators Might Do To Fix That*, VERDICT (Jan. 15, 2013), http://verdict.justia.com/2013/01/15/revenge-porn-returns-with-home-addresses.

[82] *See* Hartzog, *supra* note 81.

[83] *See* FACEBOOK FIRED, *supra* note 14 (aggregating links to stories about employees fired as a result of postings made on Facebook and other social media).

But perhaps most emblematic of attempts to violate relational boundaries is the growing trend of employers and educators requesting access to a social media user's account.[84] Not only are these employers attempting to violate technologically, legally, and normatively defined boundaries established by the user, but they are also attempting to violate the boundaries that have been set by the user's other networked connections. A fair assumption regarding the acceptance of a friendship request is that such an action only gives the identified user permission to view a friend's newly accessible profile information, particularly in light of many websites' terms of use agreements.[85]

2. *Contextual Boundaries*

Social media users also rely on contextual protections to establish boundaries, such as access controls, a limited ability to search, pseudonymity, and other obfuscating techniques to lower the likelihood that information will be found or understood.[86] In previous research, Frederic Stutzman and I have referred to the hidden context of this information as obscurity.[87] We stated: "[I]nformation is obscure online if it lacks one or more key factors that are essential to discovery or comprehension. We have identified four of these factors: (1) search visibility, (2) unprotected access, (3) identification, and (4) clarity."[88] Research has demonstrated that individuals rely almost reflexively on the obscurity created by diminishing these factors in social data.[89]

---

[84] *See* Solove, *supra* note 14 ("I thought that the practice of demanding passwords . . . was a fringe practice done by a few small companies without much awareness of privacy law. But . . . an attorney who has focused extensively on the issue, opened my eyes to the fact that the practice is much more prevalent than I had imagined . . . .").

[85] *See, e.g.*, Woodrow Hartzog, *The Problems with Requesting Access to Online Communities*, CENTER FOR INTERNET & SOC'Y (Mar. 9, 2011, 9:08 AM), http://cyberlaw.stanford.edu/blog/2011/03/problems-requesting-access-online-communities ("By asking for access to profiles, usernames, and passwords, employers and administrators aren't just asking for specific information, they are stepping into the shoes of an individual and seeing everything that individual has been authorized to see. That authorization was likely obtained through numerous negotiations (i.e. 'friend requests') whereby users rely on the representation that their 'friends' are who they say they are. . . . It is probably reasonable to assume that most Facebook users aren't contemplating a state government accessing their profile when they accept another's friend request.").

[86] *See, e.g.*, Hartzog & Stutzman, *The Case for Online Obscurity*, *supra* note 36, at 8; Hartzog & Stutzman, *Obscurity by Design*, *supra* note 36, at 387; Stutzman & Hartzog, *supra* note 69; danah boyd, *Social Steganography: Learning To Hide in Plain Sight*, ZEPHORIA (Aug. 23, 2010), http://www.zephoria.org/thoughts/archives/2010/08/23/social-steganography-learning-to-hide-in-plain-sight.html; *see also* Gelman, *supra* note 78, at 1317.

[87] Hartzog & Stutzman, *The Case for Online Obscurity*, *supra* note 36; Hartzog & Stutzman, *Obscurity by Design*, *supra* note 36.

[88] Hartzog & Stutzman, *The Case for Online Obscurity*, *supra* note 36, at 4.

[89] *Id.* at 2 n.1.

Obscurity is the result of contextual boundaries that can effectively hide social data and, as a result, keep it safe.[90] Those who use pseudonyms to check into locations using FourSquare worry less about strangers knowing their location.[91] The feeds of Twitter users with protected accounts are less likely to be scrutinized by potential employers than those with public accounts.[92] Consider the previously discussed incident with Bobbi Duncan and Taylor McCormick, in which the contextual boundary of membership in a particular group was violated when assumptions about context were incongruous with the actual visibility setting of the group.[93]

Many who interact with social data respect contextual boundaries.[94] For example, Legistorm, a website which monitors deleted tweets from politicians, has gone on the record as saying it respects users' privacy settings.[95] Because some kind of access restriction is used by most social media users in an observable way, these restrictions should be respected by those dealing with social data.[96]

Even insiders granted access to social data can now threaten contextual boundaries, as Facebook's Graph Search feature allows users to search for information that previously was protected by the high transactional cost of

---

[90] Hartzog & Selinger, *supra* note 40; NISSENBAUM, *supra* note 67, at 69–71; Finn Brunton & Helen Nissenbaum, *Vernacular Resistance to Data Collection and Analysis: A Political Theory of Obfuscation*, 16 FIRST MONDAY (May 2, 2011), http://firstmonday.org/ojs/index.php/fm/article/view/3493.

[91] *See, e.g.*, Steven Musil, *Foursquare To Show Users' Full Names, Share More Data*, CNET (Dec. 30, 2012, 9:29 AM), http://news.cnet.com/8301-1023_3-57561271-93/foursquare-to-show-users-full-names-share-more-data/.

[92] The Library of Congress did not include protected accounts in its archive of all public Twitter accounts in 2010. *See* Matt Raymond, *The Library and Twitter: An FAQ*, LIBR. CONGRESS BLOG (Apr. 28, 2010), http://blogs.loc.gov/loc/2010/04/the-library-and-twitter-an-faq/ ("Twitter's gift . . . to the Library of Congress of its entire archive of *public* tweets, announced two weeks ago today, sure has stoked the public's interest." (emphasis added)).

[93] Fowler, *supra* note 13.

[94] *See generally* NISSENBAUM, *supra* note 67.

[95] *See* Kashmir Hill, *Congressional Staffers Upset that People Actually Want To Read Their Tweets*, FORBES (Apr. 5, 2013, 2:17 PM), http://www.forbes.com/sites/kashmirhill/2013/04/05/congressional-staffers-upset-that-people-actually-want-to-read-their-tweets/.

[96] *See* MARY MADDEN ET AL., PEW RESEARCH CTR., TEENS, SOCIAL MEDIA, AND PRIVACY 2 (2013), *available at* http://www.pewinternet.org/~/media//Files/Reports/2013/PIP_TeensSocialMediaandPrivacy.pdf ("60% of teen Facebook users keep their profiles private, and most report high levels of confidence in their ability to manage their settings."); MARY MADDEN & AARON SMITH, PEW RESEARCH CTR., REPUTATION MANAGEMENT AND SOCIAL MEDIA 2 (2010), *available at* http://www.pewinternet.org/~/media//Files/Reports/2010/PIP_Reputation_Management_with_topline.pdf ("71% of social networking users ages 18–29 have changed the privacy settings on their profile to limit what they share with others online.").

visiting each profile separately to find information or by accidental (and thus less likely) discovery.[97]

3. *Temporal Boundaries*

Boundaries can also be established by the passage of time. Many kinds of social data are created for present purposes and cease to maintain this social utility once communicated, though in the world of big data, these communications might have latent value.[98] Consider one's Facebook status update announcing a job promotion or an inside joke shared with a friend on Twitter. It is unlikely the discloser and recipient will revisit those posts often (or at all) after their creation. Indeed, when Facebook first started randomly highlighting old posts, users had a negative reaction as though the past were coming back to haunt them.[99] Over time, old social data rots, gets deleted, and becomes less relevant.

The increased obscurity in this data can also serve as a kind of temporal boundary, albeit a very hazy one. After a certain amount of time, it's normatively questionable to publicize certain kinds of social data in the same way it might violate a norm for an ex-boyfriend to recount word for word an entire fight he had with his former partner ten years ago. The value of temporal boundaries was made clear in the public outcry over the Library of Congress's archiving of all public Twitter streams.[100]

Temporal boundaries are an important impetus for some versions of the "right to be forgotten" proposed in the EU and elsewhere, as well as an unresolved tension in the privacy torts between the right to free speech and the need for individuals to be able to put the past behind them.[101] It might be

---

[97] *See* Kashmir Hill, *How To Use "Graph Search" To Facebook-Stalk Mark Zuckerberg and His Employees*, FORBES (Jan. 15, 2013, 6:51 PM), http://www.forbes.com/sites/kashmirhill/2013/01/15/how-to-use-graph-search-to-facebook-stalk-mark-zuckerberg/; *see also* Harry Surden, *Structural Rights in Privacy*, 60 SMU L. REV. 1605, 1617–18 (2007).

[98] *See generally* MAYER-SCHÖNBERGER & CUKIER, *supra* note 3.

[99] *See* Mike Melanson, *Dislike Facebook's "Memorable Status Updates"?: There's a Group for That*, READWRITE (Apr. 6, 2011), http://readwrite.com/2011/04/06/dislike_facebooks_memorable_status_updates_theres#awesm=~ofb69lLReIdiWT ("Earlier this year, Facebook began testing a feature called 'Memorable Stories,' which showed users a random-seeming selection of old status updates in the site's sidebar. Within days, users began complaining that the feature showed status updates that they didn't want to be reminded of or, even worse, that deleted status updates were showing up.").

[100] *See, e.g.*, Karl Bode, *Library of Congress Responds to Privacy Gripes by Making Twitter Archive Less Useful*, TECHDIRT (May 7, 2010, 2:17 AM), http://www.techdirt.com/articles/20100503/1024339281.shtml ("Late last week a little more detail of the archiving process leaked out, the LOC saying that in response to privacy complaints they wouldn't store deleted tweets, and they'd also be placing all tweets under embargo for a period of six months . . . .").

[101] *See, e.g.*, Sidis v. F-R Publ'g Corp., 113 F.2d 806, 808–09 (2d Cir. 1940); Melvin v. Reid, 297 P. 91, 92–93 (Cal. Dist. Ct. App. 1931).

perilous to attempt to legally enforce temporal boundaries with any rigidity. Any attempt to define a temporal boundary risks being arbitrary. There is very little research to guide in the creation of determinate temporal boundaries. Yet, it appears that temporal boundaries are respected and even promoted in some contexts by those interacting with or mediating social data. For example, services that have an "exploding" feature like the popular mobile application Snapchat, which makes photos invisible after a preset time limit, inherently demonstrate that disclosures lose their primary utility as social data as time passes, even if they simultaneously gain value in a big data context.[102]

Relational, contextual, and temporal boundaries often overlap, which should be recognized by those seeking to implement the social data principles.

There are many different ways the boundary regulation principle could be implemented in the law and respected by companies and others interacting with social data. Here are three potential rules in the spirit of the boundary regulation principle:

1) There should be no coercive requests or attempts to access bound social data absent apparent permission.
2) Sensitive and confidential social data should not be disclosed outside of the boundaries in which it exists without authorization.
3) Bound social data should be left generally as obscure as it was found.[103]

B. *Those Interacting with Social Data Should Respect the Integrity of the Individual's Expressed Identity*

Identity is a central concept in social data. Erving Goffman and others have observed that identity is performative.[104] If so, there are few better stages than social media. Users craft profiles, avatars, comments, and pictures to convey "front-stage" signals—those they intend their observers to draw upon as they make sense of their information and actions.[105] In previous work, Frederic Stutzman and I have argued that "[a]ccording to Goffman, our ability to 'read' a scene, and thus appropriately judge how we present ourselves, is a critical component in social interaction. We utilize a range of cues and physical structures to figure out how we should present ourselves."[106] With regard to social data:

> On the social web, where content is peer-produced in a social milieu, new challenges of identity management have emerged. On social network sites,

---

[102] Of course, this essay has argued that big data presents related but distinct privacy-related issues.

[103] *See* Hartzog & Stutzman, *The Case for Online Obscurity*, *supra* note 36, at 2.

[104] GOFFMAN, *supra* note 23, at 22–30.

[105] *Id.*

[106] Hartzog & Stutzman, *The Case for Online Obscurity*, *supra* note 36, at 7 (citing ERVING GOFFMAN, BEHAVIOR IN PUBLIC PLACES 151–65 (1963)).

> where the articulation of the social network is a key feature, identification can occur through both direct and indirect disclosures. For example, an individual that maintains a pseudonymous profile may become publicly identifiable based on whom the individual connects to, or what a friend writes on the individual's wall. Therefore, the intention of the individual in protecting her or his identity extends beyond self-disclosure—to the management of disclosures about the individual and to the selective crafting of the online persona.[107]

danah boyd and Nicole Ellison have noted that social network sites "constitute an important research context for scholars investigating processes of impression management, self-presentation, and friendship performance."[108] Social data is used in many different ways across various platforms to create and manage identity.[109]

Disputes over identity and social data make clear the value that people place on the integrity of their identity. For example, the so-called "nymwars" involved social media restrictions on the use of pseudonyms and the mandate that users use their real names.[110] While the use of real names can help verify identity and increase user trust in the network, the inability to disguise oneself or create new identities limits the utility of social media and restricts the way in

---

[107] *Id.* at 38.

[108] boyd & Ellison, *supra* note 2, at 219; *see also id.* at 221 ("Given that [social network sites] enable individuals to connect with one another, it is not surprising that they have become deeply embedded in user[s'] lives.").

[109] *See, e.g.*, John A. Bargh et al., *Can You See the Real Me? Activation and Expression of the "True Self" on the Internet*, 58 J. SOC. ISSUES 33, 44–45 (2002); danah boyd, *Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life*, *in* YOUTH, IDENTITY, AND DIGITAL MEDIA 119, 133 (David Buckingham ed., 2008), *available at* http://mitpress.mit.edu/sites/default/files/titles/free_download/9780262524834_Youth_Identity_and_Digital_Media.pdf; Houn-Gee Chen et al., *Online Privacy Control via Anonymity and Pseudonym: Cross-cultural Implications*, 27 BEHAVIOUR & INFO. TECH. 229 (2008); Joan Morris DiMicco & David R. Millen, *Identity Management: Multiple Presentations of Self in Facebook*, *in* PROCEEDINGS OF THE ACM 2007 CONFERENCE ON SUPPORTING GROUP WORK 383, 383–86, *available at* http://dl.acm.org/citation.cfm?id=1316682; Airi Lampinen et al., *We're in It Together: Interpersonal Management of Disclosure in Social Network Services*, *in* PROCEEDINGS OF THE SIGCHI INTERNATIONAL CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 3217, 3217 (2011), *available at* http://dl.acm.org/citation.cfm?id=1979420; Airi Lampinen, Sakari Tamminen & Antti Oulasvirta, *"All My People Right Here, Right Now": Management of Group Co-presence on a Social Networking Site*, *in* PROCEEDINGS OF THE ACM 2007 CONFERENCE ON SUPPORTING GROUP WORK 281 (2009), *available at* http://www.mpi-inf.mpg.de/~oantti/pubs/fp158-lampinen.pdf. Identity has been theorized as a central aspect of privacy as well. *See, e.g.*, Jonathan Kahn, *Privacy as a Legal Principle of Identity Maintenance*, 33 SETON HALL L. REV. 371, 371–72 (2003).

[110] *See Nymwars*, WIKIPEDIA, http://en.wikipedia.org/wiki/Nymwars (last visited July 2, 2013); *see also* danah boyd, *"Real Names" Policies Are an Abuse of Power*, APOPHENIA (Aug. 4, 2011), http://www.zephoria.org/thoughts/archives/2011/08/04/real-names.html; Jillian C. York, *A Case for Pseudonyms*, ELECTRONIC FRONTIER FOUND. (July 29, 2011), https://www.eff.org/deeplinks/2011/07/case-pseudonyms.

which individuals choose to identify themselves. This interest has even been recognized by some regulators, like those in Germany, who have ordered Facebook to stop enforcing its real name policy.[111]

A related threat to the identity integrity principle is the inability to parse one's identity for diverse audiences. In previous research, Frederic Stutzman and I observed that, because individuals do not have a singular concept of identity, they often wish to bifurcate their online identity by creating two separate profiles within the same or similar media.[112] This practice preserves the integrity of our complex and often conflicting notions of identity by de-linking certain kinds of personal information from others. For example, I might like to have separate personal and professional social media accounts so that I can effortlessly share photos of me and my son dressed up as a wizard for Halloween with my personal friends and my latest publications and legal news with professional friends.

This separation is desirable not necessarily because my personal photos are private in the traditional sense of the term, but, rather, I do not wish for every aspect of my identity to be equally revealed to my friends from various different parts of my life. Such separations are seen by many organizations as wise. For example, the American Medical Association recommends separate professional and personal accounts on Facebook.[113] Yet multiple profiles are prohibited by some social network websites, including Facebook, and without the ability to cleanly manage two profiles, audience segmentation can be a cumbersome, confusing, and time consuming process.

The identity integrity principle can also be violated by those who usurp a user's identity in unacceptable ways. The most obvious example is imposters, an increasing problem for social media users that has been met with robust legislation prohibiting the practice.[114] Yet employers and other organizations

---

[111] *See* Loek Essers, *German Privacy Regulator Orders Facebook To End Its Real Name Policy*, IT WORLD (Dec. 17, 2012, 11:00 AM), http://www.itworld.com/security/328387/german-privacy-regulator-orders-facebook-end-its-real-name-policy.

[112] Stutzman & Hartzog, *supra* note 69, at 776.

[113] *See* Nicolas P. Terry, *Fear of Facebook: Private Ordering of Social Media Risks Incurred by Healthcare Providers*, 90 NEB. L. REV. 703, 713–14 (2012) ("The substantive provisions of the AMA policy relate to the privacy and confidentiality of identifiable patient data, the utilization of privacy and security settings combined with the obligation to self-audit, and the maintenance of appropriate boundaries with patients, preferably by separating the personal from the professional.").

[114] *See, e.g.*, WASH. REV. CODE ANN. § 4.24.790 (West Supp. 2013) ("A person may be liable in a civil action based on a claim of invasion of privacy when: (a) The person impersonates another actual person on a social networking web site or online bulletin board . . . ."); TEX. PENAL CODE ANN. § 33.07 (West Supp. 2012) ("A person commits an offense if the person, without obtaining the other person's consent and with the intent to harm, defraud, intimidate, or threaten any person, uses the name or persona of another person to: (1) create a web page on a commercial social networking site or other Internet website; or (2) post or send one or more messages on or through a commercial social networking site or other Internet website, other than on or through an electronic mail

also risk violating the identity integrity principle when they seek to restrict not only the professionally related activity of its agents, but also an agent's personal activity.[115]

Impersonation can create three distinct but related problems. First, the person who is being impersonated is harmed by having her identity compromised. Second, those interacting with an imposter risk being defrauded. Finally, impersonation can corrupt the integrity of an expressed social network by rendering the connections suspect and making reliance on the network dubious.

There are at least four different guidelines that can effectuate the identity integrity principle, though it is important to note that their relative desirability is entirely dependent upon the desired utility and context of the social data:

1) Restrictions on the use of pseudonyms and other identity-masking techniques should be minimized.
2) Restrictions on the use of multiple profiles and other non-deceptive audience segmentation techniques should be minimized.
3) Individuals should not be impersonated.[116]
4) There should be no undue influence exerted over an individual's online identity.

Note that the identity integrity principle is also reflected in a number of existing laws including the right of publicity and the myriad of laws prohibiting identity theft.[117] A possible tension can exist between the identity integrity principle, which seeks autonomy for individuals by allowing pseudonyms, with

---

program or message board program. (b) A person commits an offense if the person sends an electronic mail, instant message, text message, or similar communication that references a name, domain address, phone number, or other item of identifying information belonging to any person: (1) without obtaining the other person's consent . . . .").

[115] For examples, see Chris Boudreaux, *Policy Database*, SOC. MEDIA GOVERNANCE, http://socialmediagovernance.com/policies.php (last visited July 2, 2013).

[116] Obvious parody accounts, such as those that frequently appear on Twitter, would not fall into this restriction, since they would not be deceiving. *See Parody, Commentary, and Fan Account Policy*, TWITTER, https://support.twitter.com/articles/106373-parody-commentary-and-fan-accounts-policy (last visited July 2, 2013) ("Twitter users are allowed to create parody, commentary, or fan accounts (including role-playing) . . . . In order to avoid impersonation, an account's profile information should make it clear that the creator of the account is not actually the same person or entity as the subject of the parody/commentary.").

[117] *See, e.g.*, Venkat Balasubramani, *Logging into Someone Else's Facebook Account and Posting Messages on Their Friends' Walls Could Be Identity Theft*—In re Rolando S., TECH. & MARKETING L. BLOG (Aug. 1, 2011, 3:06 PM), http://blog.ericgoldman.org/archives/2011/08/california_appe.htm; Daniel Solove, *Facebook and the Appropriation of Name or Likeness Tort*, CONCURRING OPINIONS (Nov. 12, 2007, 12:27 AM), http://www.concurringopinions.com/archives/2007/11/facebook_and_th.html.

the final social data guideline, the network integrity principle, which seeks to foster and protect the trust that is established in a network.

C. *Those Interacting with Social Data Should Respect the Integrity of an Expressed Network*

The final defining characteristic of social data is the networked connection.[118] These connections can form "networked publics" with great social utility as a place to exchange opinions and useful information, provide and receive emotional support, develop a sense of self, and learn about social norms and interaction.[119] The network integrity principle is less concerned with individual harm and more concerned with protecting the trust, utility, and, if applicable, purpose of an expressed network.

There are numerous examples that demonstrate the interest in preserving network integrity. One of the most prominent recent examples is the trend of "catfishing," which one court has defined as "[t]he phenomenon of internet predators that fabricate online identities and entire social circles to trick people into emotional/romantic relationships (over a long period of time)."[120] In addition to direct harm of fraud upon the victims (a violation of the identity integrity principle), a high prevalence of imposters in a network would likely render it unreliable for many purposes.

In some networks, misrepresented identities are acceptable because pseudonyms and anonymity are the norm. However, the desire for pseudonymity is problematic when the network is designed (or mandates) "real" identities, such as with Facebook and online dating websites. For example, plaintiffs brought a lawsuit against dating website Match.com alleging, among other things, breach of contract for failing to review user profiles, failing to purge inactive profiles, falsely labeling inactive profiles as "active," failing to protect the site against scammers, and failing to verify the identities of its

---

[118] *See, e.g.*, boyd & Ellison, *supra* note 2, at 211 ("What makes social network sites unique is not that they allow individuals to meet strangers, but rather that they enable users to articulate and make visible their social networks.").

[119] *See, e.g.*, boyd, *supra* note 109, at 133; danah michele boyd, *Friendster and Publicly Articulated Social Networking*, *in* Proceedings of the ACM 2004 Conference on Human Factors in Computing Systems 1279, 1279–82 (2004), *available at* http://www.danah.org/papers/CHI2004Friendster.pdf.

[120] Zimmerman v. Bd. of Trs. of Ball State Univ., No. 1:12–cv–01475–JMS–DML, 2013 WL 1619532, at *13 (S.D. Ind. Apr. 15, 2013); *see also* Venkat Balasubramani, *Misguided Catfishing Scheme Leads to Discipline of College Students—*Zimmerman v. Ball State, TECH. & MARKETING L. BLOG (Apr. 24, 2013, 10:30 AM), http://blog.ericgoldman.org/archives/2013/04/college_student_1.htm; Bianca Bosker, *How a Tinder Experiment Lured 70 Guys to a Froyo Shop in Search of Dream Girl*, HUFFINGTON POST (Apr. 13, 2013, 5:18 PM), http://www.huffingtonpost.com/2013/04/13/tinder-experiment_n_3077047.html; Tal Z. Zarsky & Norberto Nuno Gomes de Andrade, *Regulating Electronic Identity Intermediaries: The "Soft eID" Conundrum*, 74 OHIO ST. L.J. 1335, 1371 (2013).

users.[121] The ability to trust connections within a network is crucial for many social purposes, including potentially (and perhaps ironically) the preservation of anonymity from those outside of the network.[122]

A related violation of the network integrity principle is the misappropriation of an individual's name or likeness to leverage a message to the rest of the network. For example, Facebook has settled a lawsuit claiming that the social media company misappropriated users' names and images in ads promoting its "Friend Finder" tool. "Those ads said that the user had found other friends via the friend finder tool. [Plaintiffs] argued that those messages violated California law, which provides that companies can't use the names or photos of individuals in ads without their written consent."[123] In a similar dispute, Facebook settled a lawsuit which challenged the legality of Facebook's "Sponsored Stories" program, which, according to Kashmir Hill "turns users into spokespeople for companies and products in ads that are broadcast to their friends. The disgruntled users claimed that Facebook didn't have the right to use people's names and likenesses in ads without their explicit permission."[124] These kinds of practices threaten the integrity of a network by misrepresenting the actions and intentions of other networked connections, thereby reducing overall network trust.

Another practice that threatens network integrity is mandated networked connections. For example, in trying to resolve evidentiary disputes involving social media, some judges have suggested "friending" to get access to the requested data.[125] Some organizations have asked members to "friend" human

---

[121] Robinson v. Match.com, Nos. 3:10–CV–2651–L, 3:11–CV–1354–L; 3:11–CV–1913–L; 3:11–CV–02319–L; 3:11–CV–02322–L; and 3:11–CV–02323–L, 2012 WL 3263992, at *4 (N.D. Tex. Aug. 10, 2012); *see also* Venkat Balasubramani, *Lovelorn Plaintiffs Strike Out Against Match.com*—Robinson v. Match.com, TECH. & MARKETING L. BLOG (Sept. 30, 2012, 12:12 PM), http://blog.ericgoldman.org/archives/2012/09/lovelorn_plaint.htm.

[122] *See* Hal Hodson, *Facebook Could Help Hide Your Identity*, GIZMODO (Sept. 14, 2012, 6:11 AM), http://gizmodo.com/5943249/how-facebook-could-help-hide-your-identity.

[123] Wendy Davis, *Facebook, Consumers Settle "Friend Finder" Dispute*, ONLINE MEDIA DAILY (Sept. 14, 2012, 5:58 PM), http://www.mediapost.com/publications/article/182974/facebook-consumers-settle-friend-finder-dispute.html#axzz2WCvGuQqq.

[124] Kashmir Hill, *Facebook Will Pay $10 Million To Make Its "Sponsored Stories" Problem Go Away*, FORBES (June 18, 2012, 11:45 AM), http://www.forbes.com/sites/kashmirhill/2012/06/18/facebook-will-pay-10-million-to-make-its-sponsored-stories-problem-go-away/.

[125] *See, e.g.*, Venkat Balasubramani, *Judge Offers To Facebook "Friend" Witnesses in Order To Resolve Discovery Dispute*—Barnes v. CUS Nashville, TECH. & MARKETING L. BLOG (June 9, 2010, 10:56 AM), http://blog.ericgoldman.org/archives/2010/06/judge_offers_to.htm. *But see* Venkat Balasubramani, *Plaintiff Can't Be Forced To Accept Defense Counsel's Facebook Friend Request in Personal Injury Case*—Piccolo v. Paterson, TECH. & MARKETING L. BLOG (May 19, 2011, 8:30 AM), http://blog.ericgoldman.org/archives/2011/05/court_says_plai.htm.

resource directors.[126] Such mandates can have the effect of corrupting the trust that other individuals place in the network.

The inverse practice of banning networked connections could also corrupt the integrity of a network by limiting its growth. For example, the Missouri State Senate proposed a bill that would forbid students and teachers being Facebook friends.[127] That aspect of the bill was later deemed problematic and was amended, which demonstrates, among other things, the societal interest in supporting the network integrity principle.[128]

Asking friends to betray trust put in others can also be seen as a network corruption. In September 2012, Facebook users were surprised to see a notification box which displayed a picture of a user's "friend" and asked if that user was using his real name in accordance with Facebook's "real name" policy.[129] One critic referred to the tactic and resulting dispute as "snitchgate," while Facebook clarified that it only wanted to gather anonymous information about how the website was used, stating, "[w]e are always looking to gauge how people use Facebook and represent themselves to better design our product and systems. We analysed these surveys only using aggregate data and responses had zero impact on any user's account."[130] The public's resistance to being asked to report whether their networked connections are violating a social network site's terms of use agreement would seem to demonstrate the existence and desirability of trust within a network. Finally, unauthorized surveillance can threaten the integrity of a network for the same general reasons surveillance is problematic, with the added reason that, if discovered, trust in the network will be eroded.[131]

Potential rules or guidelines to effectuate the network integrity principle include:

1) There should be no misrepresentations made to induce reliance on a false identity of a networked connection.

---

[126] *See* Erik Sherman, *Required To "Friend" the Boss on Facebook? More States Say No*, AOL JOBS (June 7, 2013, 6:01 AM), http://jobs.aol.com/articles/2013/06/07/friend-the-boss-facebook-laws/ ("According to the Council of State Governments, some companies are asking employees to '"friend" a human resources director or coach.' And many workers are, understandably, nervous.").

[127] *See, e.g.*, Charlie White, *Missouri Forbids Teachers and Students To Be Facebook Friends*, MASHABLE (July 30, 2011), http://mashable.com/2011/07/30/student-teacher-facebook/.

[128] *See* Emil Protalinski, *Missouri Senate Lets Teachers Be Facebook Friends with Students*, ZDNET (Sept. 15, 2011, 9:43 AM), http://www.zdnet.com/blog/facebook/missouri-senate-lets-teachers-be-facebook-friends-with-students/3687.

[129] *See* Kashmir Hill, *Facebook Stops Asking Users To "Snitch" on Friends with Fake Names*, FORBES (Sept. 24, 2012, 12:00 PM), http://www.forbes.com/sites/kashmirhill/2012/09/24/facebook-stops-asking-users-to-snitch-on-friends-with-fake-names/.

[130] *Id.*

[131] *See* Neil Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1934–35 (2013).

2) A networked connection's name or likeness should not be used without consent to imply an endorsement of a third-party's message to the network.
3) There should be no unauthorized or hidden surveillance of a bound network.
4) There should be no mandate or prohibition of networked connections.

The three principles identified here—boundary regulation, identity integrity, and network integrity—cannot address every problematic aspect of the social web. They are proposed merely as a common language and a set of general policy objectives for stakeholders interacting with social data as the front stage of the Internet.

A common language and articulation of policy objectives have been missing in the amorphous and ill-defined context of the social web. This lack of guidance is now becoming problematic with the growing necessity and reality of government and organizational regulation of social data. While the proposed principles have overlapping aspects, they are distinct enough to provide nuance in discussions regarding the proper way to work with social data. The question that remains, then, is how these principles might be implemented.

IV. IMPLEMENTING THE SOCIAL DATA PRINCIPLES

Like the FIPPs, the social data principles proposed in this essay are not designed to be self-enforcing. Rather, they may be enforced or implemented in various different ways at the statutory, regulatory, common law, and organizational levels. The principles may be used to provide protection that is tailored to specific contexts and the particular needs and capabilities of organizations and individuals and should account for conflicting goals and tolerable cost of implementation.

Robert Gellman has commented on the diverse ways in which the FIPPs may be implemented, and the same holds true for the social data principles, stating that "accountability can be met through many different mechanisms, including criminal or civil penalties; national or provincial supervisory officials; other administrative enforcement; various forms of self-regulation including industry codes and privacy seals; formal privacy policies; compliance audits; employee training; privacy officers at the data controller level; and other methods."[132]

The need to implement the social data principles can arise with any organization that might be working with social data or when a practice becomes problematic enough that regulatory guidance or prohibitions become

[132] Gellman, *supra* note 1, at 23.

necessary.[133] Regardless of the regulatory mechanism, the social data principles may be or are already being effectuated in four general ways: 1) disclosure limitations, 2) design, 3) limitations on the use of social technologies, and 4) limitations on requests for social data.

A. *Disclosure Limitations*

One of the most common ways to protect social data is to restrict authorized recipients of social data from further disclosure. The most significant example of this kind of limitation is the law of confidentiality, which is a central component of many torts, statutes, regulations, contracts, evidentiary privileges, professional codes, and company policies.

Confidentiality law is largely aimed at enforcing respect for relational boundaries. That is, confidants are usually obligated to refrain from disclosing a particular piece of information to other people outside of a confidential relationship. However, disclosure limitations can also be crafted to respect contextual and temporal boundaries as well. Those seeking to enforce the boundary regulation principle could reinforce contextual boundaries by restricting the disclosure of social data to certain contexts or keeping information obscure. Agreements could allow certain disclosures so long as they do not make information searchable or publicly accessible, identify the discloser or subject, or clarify an opaque piece of information. In this way, restrictions need not be absolute and can provide for dissemination to some, but not others (or all). Alternatively, as social data ages, recipients could be increasingly restricted in their disclosures in order to respect temporal boundaries. As is the case with other forms of confidentiality, more burdensome restrictions could be limited to particular, sensitive kinds of data.

B. *Design*

In many contexts, it might make more sense to implement the social media principles through design. For example, Bobbi Duncan and Taylor McCormick were outed as a function of Facebook's privacy settings. The settings, of course, could have been changed to make the group membership private, yet many users, including the creator of the Queer Choir Facebook Group, have been confused by increasingly complex privacy settings.[134] The social data principles could guide the design of these settings to make the data-protective choices more intuitive for users.

---

[133] *See, e.g.*, Hunton & Williams LLP, *FFIEC Issues Draft Guidance on Social Media*, PRIVACY & INFO. SECURITY L. BLOG (Jan. 25, 2013), http://www.huntonprivacyblog.com/2013/01/articles/ffiec-issues-draft-guidance-on-social-media/.

[134] *See* Johnson et al., *supra* note 34; Michelle Madejski et al., A Study of Privacy Settings Errors in an Online Social Network (presented at the Fourth International Workshop on SECurity and SOCial Networking, Mar. 19, 2012), *available at* https://www.cs.columbia.edu/~smb/papers/fb-violations-sesoc.pdf.

Many already consider the protection of information a design issue with policy implications. Privacy by Design, that is "the philosophy and approach of embedding privacy into the design specifications of various technologies," seeks to build "the principles of Fair Information Practices . . . into the design, operation and management of information processing technologies and systems."[135] In 2012, the Federal Trade Commission (FTC) privacy framework, *Protecting Consumer Privacy in an Age of Rapid Change*, strongly encouraged companies to adopt privacy-by-design approaches to their business and technical operations.[136]

Social data principles could also be implemented by privacy enhancing technologies, known as PETs.[137] For example, YouTube's face-blurring tool allows users to obfuscate their identity, which is consistent with the identity integrity principle.[138]

C. *Limitations on Use of Social Technologies*

Many of the social data principles could be effectuated not by limiting the disclosure of certain kinds of information, but, rather, by limiting the use of the technology used to create that data. Laws and policies could prohibit imposters, forced "friends," misappropriation of name or likeness, and unauthorized surveillance.

Many of these restrictions are common in workplace and academic social media policies.[139] They are also routinely prohibited in social media's terms of use. For example, in Facebook's "Statement of Rights and Responsibilities," users are not allowed to

> bully, intimidate, or harass any user . . . tag users or send email invitations to non-users without their consent . . . use Facebook to do anything unlawful, misleading, malicious, or discriminatory . . . provide any false personal information on Facebook . . . [or] post content or take any action on Facebook that infringes or violates someone else's rights or otherwise violates the law.[140]

---

[135] CAVOUKIAN, *supra* note 20, at 1; *see* ANN CAVOUKIAN, PRIVACY BY DESIGN: THE 7 FOUNDATIONAL PRINCIPLES (2009), *available at* http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf; Rubinstein, *supra* note 20, at 1421 ("Privacy by design is an amorphous concept."); Rubinstein & Good, *supra* note 20, at 4.

[136] FTC, *supra* note 20, at vii.

[137] *See* Yang Wang & Alfred Kobsa, *Privacy-Enhancing Technologies*, *in* HANDBOOK OF RESEARCH ON SOCIAL AND ORGANIZATIONAL LIABILITIES IN INFORMATION SECURITY 203 (Manish Gupta & Raj Sharman eds., 2006); John Argyrakis et al., *Privacy Enhancing Technologies: A Review*, *in* ELECTRONIC GOVERNMENT 282 (Roland Traunmüller ed., 2003).

[138] Zoe Fox, *YouTube Releases Face-Blurring Tool for Editing Graphic Footage*, MASHABLE (July 18, 2012), http://mashable.com/2012/07/18/youtube-face-blur/.

[139] *See* Boudreaux, *supra* note 115.

[140] *Statement of Rights and Responsibilities*, FACEBOOK, https://www.facebook.com/legal/terms (last visited July 2, 2013).

D. *Limitations on Requests for Social Data*

Finally, the principles could be effectuated by limiting requests for social data. Such limitations are also commonly found in terms of use agreements. For example, in Facebook's "Statement of Rights and Responsibilities," users are not allowed to "solicit login information or access an account belonging to someone else."[141] Legislators are also passing laws in the spirit of this guideline. Consider the previously mentioned spate of proposed and passed legislation that prevents employers and school administrators from requesting usernames and passwords and access to social media accounts.[142] More controversially, the ACLU brought a lawsuit in November 2012 "to block a ballot measure that would require sex offenders to turn over information about their Internet accounts to police."[143]

Whereas disclosure limitations limit what "insiders" can do with social data, this method of implementation applies primarily to "outsiders" seeking social data. It supports both the boundary regulation principle, to the extent the boundaries set by the user render social data inaccessible to outsiders, as well as the network integrity principle by helping to maintain a sense of trust in the network.

V. CONCLUSION

It is increasingly important to distinguish between the different threats to privacy that arise from the conversion of our social interactions into data. The regulatory and self-regulatory response to the "backstage" threat posed by electronic databases developed partially thanks to the common language and framework of the Fair Information Practice Principles. Yet, those seeking to disclose and access information from the "front stage" of the social web, the user interface, have no such guidelines to look to. This essay has proposed a set of guiding principles for the protection of social data, the Boundary Regulation Principle, the Identity Integrity Principle, and the Network Integrity Principle. These principles could be implemented through various regulatory and self-regulatory efforts, including limitations on disclosure and use of the data, limitations on requesting the data, and via design strategies.

Due to the extreme messiness of social interaction, the principles are destined to remain imperfect and, at times, even internally conflicting. Yet if the relevant stakeholders were to draw upon a set of common principles, they would be better able to identify, justify, and distinguish between proposed

---

[141] *Id.*

[142] *See supra* Part II.B.

[143] Brendan Sasso, *ACLU Sues To Protect Online Privacy of Sex Offenders*, HILL (Nov. 7, 2012, 4:31 PM), http://thehill.com/blogs/hillicon-valley/technology/266671-aclu-%20sues-to-protect-online-privacy-of-sex-offenders#ixzz2WJLsfjYe.

social data protections, which are important as our social interactions increasingly endure.